Maturity Level Analysis of Inventory Information Systems Using COBIT 4.1 Framework at PT. MEDISTA UTAMA

Susi Susilowati

Universitas Bina Sarana Informatika, Indonesia

susi.sss@bsi.ac.id

Abstract

PT. Medista Utama is a company engaged in the distribution of medical devices. We have implemented an information system in the inventory section that is used to control the movement of products in the company. The system used must be able to manage, convey and maintain information security properly. So it is necessary to carry out an audit that aims to evaluate the information system governance that is running and ensure that the existing procedures support the existing business processes in the company. The audits were conducted following the standards of the COBIT 4.1 Framework for IT governance. This study will focus on the Delivery Service and Support (DSS) domain to analyze several aspects of IT that are currently running in this company, from the level of system security used to the management carried out by the system. In this domain, the research is focused on the DS5, DS10, and DS11 sub-domains. From the research results it is known that DS5 is at the level of 1.3; DS10 and DS11 are at level 2 (Repetitive but Intuitive). The conclusion is the level of capability obtained from the inventory information system of PT. Medista Utama is still below the expected level. And many improvements are needed to maximize the company's performance to achieve the expected Maturity Level value.

Keywords: Inventory, Cobit 4.1, Maturity Level, Delivery Service and Support

1. Introduction

The development of Information Systems is now so fast, using the media, including information technology such as the internet, desktop applications and so on, this information through the media can be conveyed to reach various parts of society. The availability of a good and reliable information system is increasingly felt to be important in line with the increasing human need for fast, precise, and accurate information. Information that has been obtained late or the level of its accuracy is questionable not only makes it difficult for a person or an institution to make decisions but also can bring huge losses to many parties [1]. By taking advantage of advances in science and technology. Management of data that is more effective and efficient with a computerized work system will greatly assist in building a good and reliable information system, to meet information needs that are faster, more precise, and accurate [1]. Information itself is data that has been processed, so it is useful for making decisions. In other words, information is a fact that has meaning and is useful for achieving certain goals. Information is different from data because the information is the final result or output of an information system. Good information is information that is provided regarding matters that are relevant only.

PT. MEDISTA UTAMA is engaged in the distribution of medical devices. Inventory data management system at PT. MEDISTA UTAMA still uses an offline system where users who use this system can only access media that the system has installed itself on. The problem found in the management of information systems in this company is inaccurate data (data in the system is not the same as actual/physical). One of the causes
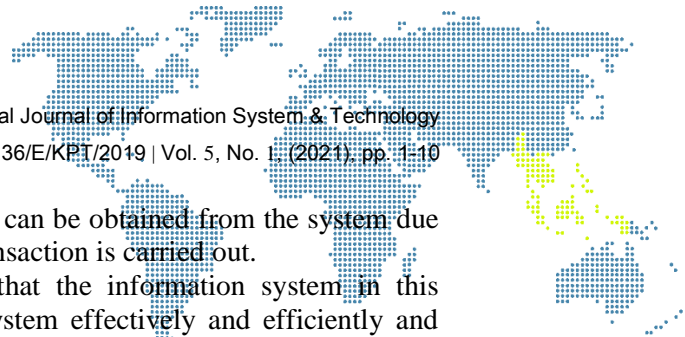
of this inaccuracy is the incomplete information that can be obtained from the system due to the limited input of information at the time the transaction is carried out.

Information system audit functions to ensure that the information system in this company safeguards information assets uses the system effectively and efficiently and maintains integrity [2]. The purpose of this study is also to assess the current level of capability to achieve the target capability level that has been targeted by the company. To audit the performance of a company's information system in this study, researchers used COBIT 4.1 (Control Objectives for Information and Related Technologies) by focusing on the DS5, DS10, and DS11 sub-domains.

2. Research Methodology

The research conducted and the author's stages in taking or obtaining data from sources, starting from the initial survey, interviews, and questionnaires are shown in the following research flowchart.
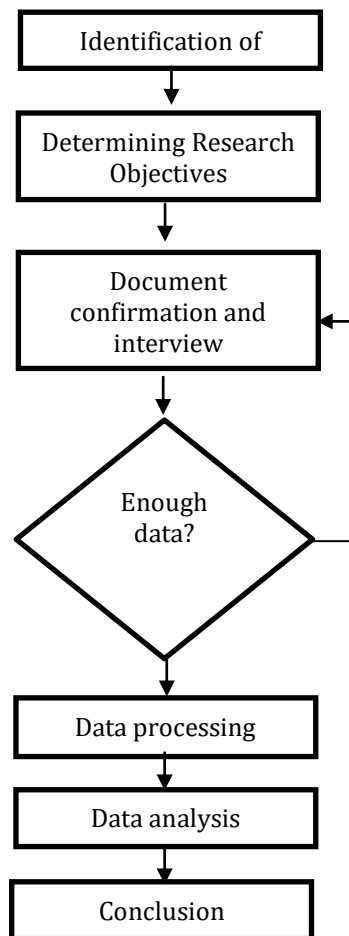

Figure 1. Research Flowchart

Research Procedure is an activity that must be carried out in conducting research. The stages and research procedures are as follows:

a) Planning(Planning)

Planning is the initial stage in the research procedures we carry out. Because at this stage we can determine the scope, an object to be audited, the evaluation standard of the audit results, and communication to the person concerned about the organization/company to be audited by analyzing a vision, mission, goals, and objectives of the object, and policies related to investigative processing. The design stage includes several main activities, namely determining the scope and objectives

of the audit, organizing the audit team, understanding the client's business operations, reviewing previous audit results, and preparing an audit program.

b) Field Work(Field Inspection)

At this stage, the auditor aims to obtain information by collecting data with related parties using several methods that can be done, such as; interviews, questionnaires, and conduct direct surveys to the place where the research was conducted. The data obtained later will be very useful in helping auditors to analyze an organization/company being audited.

c) Reporting(Reporting)

After the data collection process, the data will be processed to be calculated based on the maturity level calculation. At this stage what the auditor will do is provide information in the form of the results of the audit. The calculation of the maturity level is carried out by referring to the results of interviews, surveys, and the recapitulation of the results of distributing questionnaires. Based on the results of the maturity level that reflects the current performance (current maturity level) and the standard or ideal performance which is expected to become a reference for further analysis of the gap (gap). This is intended to identify gaps and find out what causes these gaps. With reporting, a problem can be seen more clearly where the error lies.

d) Follow-Up (Follow-up)

After reporting or reporting, the next thing to do is to provide a report on the results of the audit in the form of recommendations for corrective actions to the management of the object under study, and then the improvement authority is the responsibility of the management of the object under study whether it will be implemented or only as a reference for improvement in the future.

2.1. Audit

Information Systems Audit is a process for collecting and evaluating evidence in determining whether an information system has been built to maintain data integrity, safeguard assets, make organizational goals can be achieved effectively, and use resources efficiently [3]. With the introduction of COBIT, now the objective of auditing is not only limited to the classic concept, but now it is the effectiveness, efficiency, confidentiality, integrity, availability, compliance with policies/rules, and reliability of information systems. In practice, this type of audit develops in several variants [4]:

a) Operational audit (operational audit) of the management of the information system, or more precisely/strictly on information technology governance (IT governance),

b) General information review, an audit of general information systems in a particular organization,

c) An audit of a specific application under development (quality assurance at the system development stage).

2.2. Inventory

Inventory is the material used by a company to run its business. If the company produces a good or service, the material is used to support or provide production needs. Inventory for the company is to anticipate customer needs [5].

2.3. Application

In terms of the definition of an application is a program that is ready to use which is made to carry out a function for application service users as well as the use of other applications that can be used by a target to be addressed. According to the executive computer dictionary, applications have the meaning of solving problems that use one of the application data processing techniques that usually race against a desired or expected computation and expected data processing. Understanding the application according to the
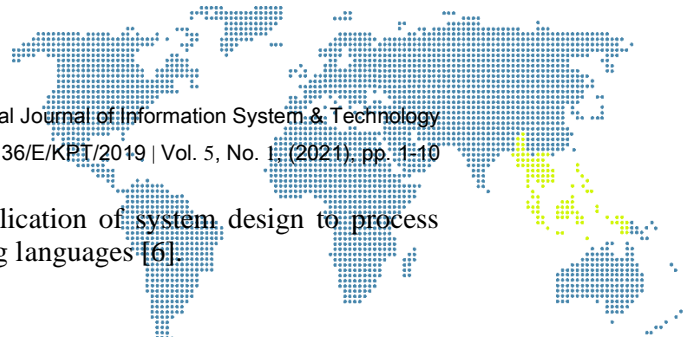
Big Indonesian Dictionary, "Application is the application of system design to process data using rules or provisions of certain programming languages [6].

2.4. COBIT Framework

COBIT (Control Objective for Information and related Technology) is a framework consisting of domains and processes used to manage activities and logical structures [7]. Overall Framework COBIT 4.1 can be seen in Figure 3. There are 4 main domains in the COBIT 4.1 Framework, namely [8]:

a) Planning and Organization (PO)
   This domain includes strategy and tactics, and concerns identifying how IT can optimally contribute to the achievement of business goals. In addition, the realization of the strategic vision needs to be planned, communicated, and managed from different perspectives. Thus, an organizational and technological infrastructure must be put in place.

b) Acquisition and Implementation (AI)
   To realize an IT strategy, IT solutions need to be identified, developed or acquired and implemented, and integrated into business processes. In addition, changes, and maintenance of existing systems must be covered in this domain to ensure that the life cycle will continue for this system.

c) Delivery and Support (DS)
   This domain focuses primarily on the delivery/delivery aspect of IT. This domain includes areas such as the operation of applications in IT systems and their results, as well as, the support processes that enable the effective and efficient operation of these IT systems. This support process includes security issues/concerns as well as training.

d) Monitoring and Evaluation (ME)
   All IT processes need to be assessed regularly overtime to maintain quality and compliance with control requirements. This domain points to the need for management oversight of the control process within the organization as well as independent assessments carried out by both internal and external auditors or obtained from other alternative sources.

2.5. Maturity Level

The generic maturity model used is:

a) Non-existent - There are no visible processes at all. The company hasn't realized that there is a problem to have studied.

b) Initial/Ad Hoc - There is evidence that the company is aware of the problem and should be assessed but there is no standardization yet. However, there is an ad hoc approach that tends to be applied on a case-by-case basis. Management's approach is generally unstructured.

c) Repeatable but Intuitive - The process has been developed at a stage where a similar procedure has been followed by various people carrying out this task. There is no formal training or communication about standard procedures and the responsibility falls on the individual. There is high dependence on the individual and frequent errors.

d) Defined Process - Standardized and documented procedures, and communication through training. This process must be followed. However, a slight deviation occurs. The procedure is not complicated but the formalization of current practice

e) Managed and measurable - Management monitors and measures compliance with procedures and takes actions where processes appear to be ineffective. The process is developed on an ongoing basis and provides good practice. Automation and tools are used in limited and fragmented ways.

f) Optimized - The process has been designed to a good level of implementation, based on the results of continuous development and maturity modeling with other
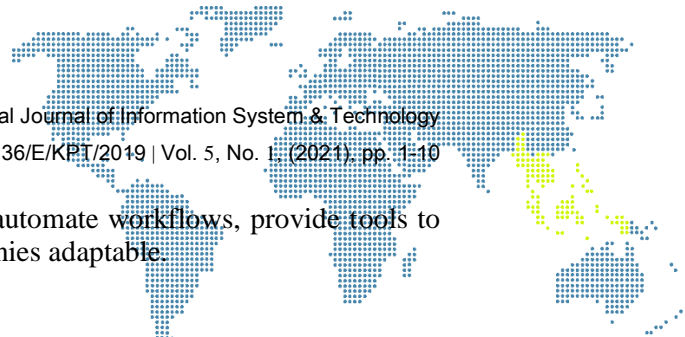
companies. IT is used in an integrated way to automate workflows, provide tools to improve quality and effectiveness, make companies adaptable.

3. Results and Discussion

This section, it discusses the inventory information system with the COBIT framework at PT. MEDISTA UTAMA. Here, we analyze several aspects of IT that are currently running in this company, starting from the level of system security that is used to the management that is carried out by the system.

3.1. Ensure Security System

The need to maintain information integrity and protect IT assets requires a security management process. This process includes building and maintaining IT, security roles and responsibilities, policies, standards, and procedures. Security management also includes conducting periodic security monitoring and testing and implementing corrective actions to identify security weaknesses or incidents. Effective security management protects all IT assets to minimize the business impact of security vulnerabilities and incidents, here is the definition of its sub-domains [6].

Sub Domain Ensure Security System:

a) DS 5.1 Management of IT Security:
    Manage IT security at the organizational level as high as possible, so that security management actions are in line with business requirements.

    Findings of DS 5.1 Management of IT Security:
    PT. MEDISTA UTAMA has a standard security system and does not pay attention to the strict security system.

b) DS 5.3 Identity Management:
    Ensure that all users (Internal, External, and temporary) and their activities in the use of the IT system can be identified. Allows user identification via an authentication mechanism. Confirm that only certain users can access important data.

    Findings of DS 5.3 Identity Management :
    From the results of the interview, the information system PT. MEDISTA UTAMA only has employee accounts

c) DS 5.4 User Account Management:
    Can do Address requesting, establishing, issuing, suspending, modifying, and closing all privileged accounts and accounts with one main account that governs the account management.

    Findings of DS 5.4 User Account Management
    From the results of the interview, PT. MEDISTA UTAMA does not have a special account to manage other accounts.

d) DS 5.9 Malicious Software Prevention, Detection, and Correction:
    Take preventive action, perform early detection, on systems used to protect data and technology from malware attacks (Viruses, Worms, Spyware, Spam).

    Findings of DS 5.9 Malicious Software Prevention, Detection, and Correction
    From the results of the interview, PT. MEDISTA UTAMA properly maintains the PC used from various malware, and always updates its security.

e) DS 5.10 Network Security:
    Use security techniques such as firewalls, security appliances, network segmentation, intrusion detection to authorize access and control the flow of information from the network to the network.

    Findings of DS 5.10 Network Security
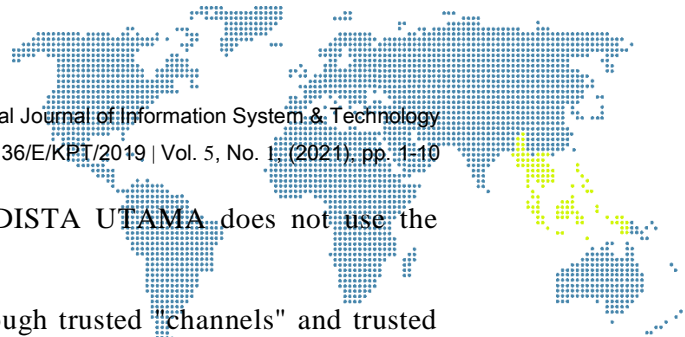
From the results of the interview, PT. MEDISTA UTAMA does not use the internet network to run system applications.

f) DS 5.11 Exchange of Security Data:

Process important data transactions only through trusted "channels" and trusted media that can provide control over the authenticity of goods, proof of submission, proof of receipt.

Findings of DS 5.11 Exchange of Security Data

From the results of the interview, PT. MEDISTA UTAMA only uses applications in making transactions.

3.2. Analysis Results

a) PT. MEDISTA UTAMA does not have an adequate standard procedure for Maturity Level 3, and the result is Maturity Level 1 because it does not have an adequate security system.

b) PT. MEDISTA UTAMA does not have adequate standard procedures for Maturity Level 3, and the result is Maturity Level 1 because the management of system application accounts can be done by every employee.

c) PT. MEDISTA UTAMA does not have adequate standard procedures for Maturity Level 3, and the result is Maturity Level 1 because there is no main account that can manage the accounts used.

d) PT. MEDISTA UTAMA does not have adequate standard procedures for Maturity Level 3, and the result is Maturity Level 2 because of PT. MEDISTA UTAMA has used a variety of software to secure its PC from various malware and periodically updates the software used.

e) PT. MEDISTA UTAMA does not have adequate standard procedures for Maturity Level 3, and the result is Maturity Level 1 because of PT. MEDISTA UTAMA does not use the internet network to run its system applications so that data storage and application flexibility to be accessed is limited.

f) PT. MEDISTA UTAMA does not have an adequate standard procedure for Maturity Level 3, and the result is Maturity Level 1 because in the system application management transaction at PT. MEDISTA UTAMA can only be done on a computer/device that has installed the application and is connected to the database which is stored in storage so that it cannot be accessed from a device that does not have the application.

From the results of the audit analysis, the Maturity Level obtained from each sub-domain in the DS 5 Ensure Security System and the results of the process can be seen in table 1 of the Ensure Security System.

Table 1. Ensure Security System

No.	Sub Domain	Current	Expected
DS 5.1	Management of IT Security	1	3
DS 5.3	Identity Management	1	3
DS 5.4	User Account Management	1	3
DS 5.9	Malicious Software Prevention, Detection, and Correction	2	3
DS 5.10	Network Security	1	3
DS 5.11	Exchange of Security Data	1	3

3.3. Manage Problems

Effective problem management requires problem identification and classification, root cause analysis, and problem-solving. The problem management process also includes the formulation of recommendations for improvement, maintenance of problem records, and review of the status of corrective action. Effective problem
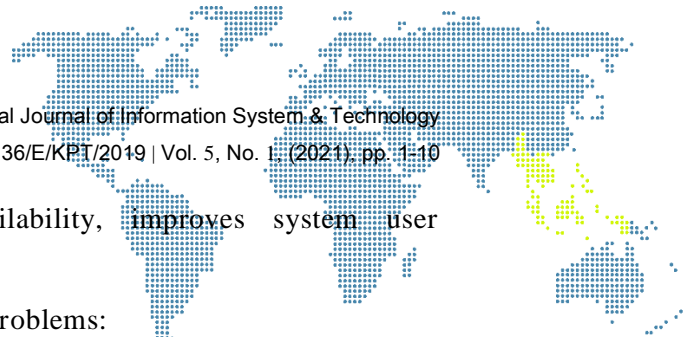
management process maximizes system availability, improves system user convenience.

Definition of Sub Domain Management Problem:

a) DS 10.1 Identification and Classification of Problems:

Implement a process for reporting and classifying known issues as part of incident management. The steps used to classify the problem are the same as the steps for classifying incidents. These problems are categorized by the category of impact, urgency, and priority.

Findings of DS 10.1 Identification and Classification of Problems

From the findings, PT. MEDISTA UTAMA can properly identify, classify problems that occur in its business from previous experiences.

b) DS 10.2 Problem Tracking and Resolution:

Ensure that the problem management system provides everything for the proper audit, facilities that allow tracking, analyzing, and determining the root cause of all issues reported. Identify and carry out ongoing problem-solving solutions to solve the problem to its core.

Findings of DS 10.2 Problem Tracking and Resolution

From the findings, PT. MEDISTA UTAMA can analyze the problems that occur, managers and staff, discuss how these problems occur, and find out the root of the problem.

c) DS 10.3 Problem Closure:

Put in place procedures to close the problem log either after reports that the problem has been resolved or after agreeing with the business on alternative ways of resolving the problem.

Findings of DS 10.3 Problem Closure

From the findings, PT. MEDISTA UTAMA can solve the problems that occur with the best solution with a win-win condition for both parties, for example, as replacement of damaged goods.

3.4. Analysis Results

a) PT. MEDISTA UTAMA does not have an adequate standard procedure for Maturity level 3 and the result is Maturity Level 2 because the management held discussions with staff to identify the problems faced and classify the impact of these problems.

b) PT. MEDISTA UTAMA does not yet have an adequate standard procedure for Maturity level 3 and the result is Maturity Level 2 because the management held discussions with staff to find the source of the error and how it could happen.

c) PT. MEDISTA UTAMA does not have adequate standard procedures for Maturity level 3 and the result is Maturity Level 2 because the management can solve it with the best solution with a win-win solution between the customer and the management.

From the results of the audit analysis, the Maturity Level of each sub-domain in DS 10 Manage Problems is obtained and the results of the process can be seen in Table 2 Manage Problems.

Table 2. Manage Problem

No.	Sub Domain	Current	Expected
DS 10.1	Identification and Classification of Problems	2	3
DS 10.2	Problem Tracking and Resolution	2	3
DS 10.3	Problem Closure	2	3
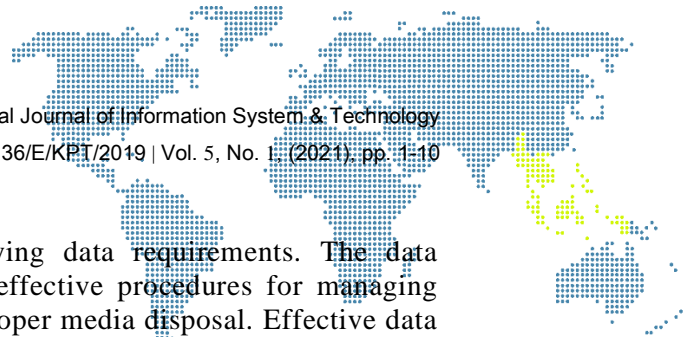
3.5. Manage Data

Effective data management requires identifying data requirements. The data management process also includes establishing effective procedures for managing media libraries, data backup and recovery, and proper media disposal. Effective data management helps ensure the quality, timeliness, and availability of business data.

Definition of Sub Domain Manage Data:

a) DS 11.3 Media Library Management System:

Establish and implement procedures for maintaining inventory media storage and archiving uses and integrity.

> Findings of DS 11.3 Media Library Management System
>
> From the results of the interview with PT. MEDISTA UTAMA has a way of securing important storage media and archives for its business.

b) DS 11.4 Disposal:

Establish and implement procedures to ensure that business requirements for the protection of sensitive data and software are met when data and hardware are disposed of or transferred.

> Findings of DS 11.4 Disposal
>
> From the results of interviews with PT. MEDISTA UTAMA, we have a habit of securing all important data before transferring data.

c) DS 11.5 Backup and Restoration:

Establish and implement procedures for backup and system recovery, applications, data, and documentation by business requirements and continuity plans.

> Findings of DS 11.5 Backup and Restoration
>
> From the results of interviews with PT. MEDISTA UTAMA always backing up data within a certain period time to ensure the data is always updated.

d) DS 11.6 Security Requirements for Data Management:

Establish and implement policies and procedures to identify and implement applicable security requirements for the reception, processing, storage, and output of data to meet business objectives, organizational security policies, and regulations.

> Findings of DS 11.6 Security Requirements for Data Management
>
> From the results of interviews with PT. MEDISTA UTAMA to implement security to protect the data, such as certain data can only be accessed by staff who are given permission to access the system.

3.6. Analysis Results

a) PT. MEDISTA UTAMA does not have adequate standard procedures for Maturity level 3 and the result is Maturity Level 2 because management already has a way to secure storage media and important records for its business.

b) PT. MEDISTA UTAMA does not have adequate standard procedures for Maturity level 3 and the result is Maturity Level 2 because of PT. MEDISTA UTAMA has the habit of securing important data before transferring data.

c) PT. MEDISTA UTAMA does not yet have adequate standard procedures for Maturity Level 3 and the result is Maturity Level 2 because the management has the habit of doing data backups and updating periodically.

d) PT. MEDISTA UTAMA does not have adequate standard procedures for Maturity level 3 and the result is Maturity Level 2 because of PT. MEDISTA UTAMA applies a regulation whereby not all staff working in the company can access data on the system.

From the results of the audit analysis, the Maturity Level of each sub-domain in DS 11 Manage Data is obtained and the results of the process can be seen in Table 3 Manage Data.
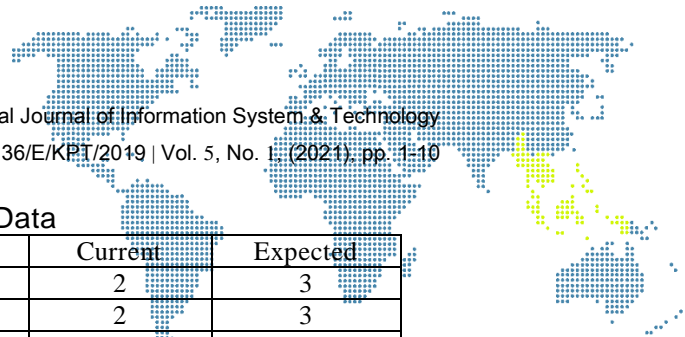
Table 3. Manage Data

No.	Sub Domain	Current	Expected
DS 11.3	Media Library Management	2	3
DS 11.4	Disposal	2	3
DS 11.5	Backup and Restoration	2	3
DS 11.6	Security Requirements for Data Management	2	3

3.7. Results of Recapitulation and Recommendations

From the audit results above, the average sub-domain of the maturity level calculation results is shown in Table 4 Recapitulation of the Average Maturity Level Calculation Results.

Table 4. Recapitulation

No.	Sub Domain	Current	Expected
DS 5	Ensure Security System	1.3	3
DS 10	Manage Problems	2	3
DS 11	Manage Data	2	3
Average		1.76	3

The results of the audit show that the current (currently) has not yet reached the expected value, so we have prepared several recommendations to achieve the expected value.

3.8. DS 5 Ensure Security System

We provide recommendations for PT. MEDISTA UTAMA as follows:
a) Using better antivirus software and always updating it regularly.
b) Ensuring important data is not accessed or stolen by other people, for example by using private system access to add data security.
c) Implementing an accounting identity so that managers can monitor which staff is accessing data
d) Add the main account that can perform management actions on other accounts

3.9. DS 10 Manage Problems

We provide recommendations for PT. MEDISTA UTAMA as follows:
a) Implementing formal procedures, where staff follow these procedures to identify and classify the problems they face so that the actions taken are more consistent.
b) Implementing a formal procedure, where staff follows these procedures to analyze the problems they are facing and how to find the root of the problem so that the actions taken are more consistent.
c) Implement formal procedures, where staff follows these procedures to solve problems with the best solution so that the actions taken are more consistent.

3.10. DS 11 Manage Data

We provide recommendations for PT. MEDISTA UTAMA as follows:
a) Implementing formal procedures, where staff follow these procedures to maintain an inventory of data storage, to avoid things that are not desired
b) Implement a formal procedure, where staff follow these procedures to secure data before data is transferred to another device. to avoid things that are not desirable
c) Implement a formal procedure, where staff follows these procedures to ensure the backup and system recovering process runs properly and there are no disruptions so that the actions taken are more consistent.
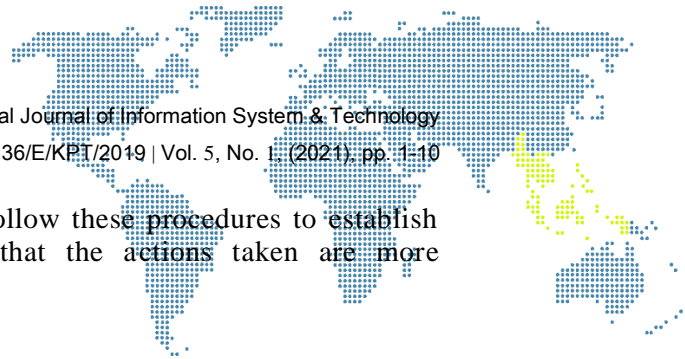
d) Implement formal procedures, where staff follow these procedures to establish policies for processing data received so that the actions taken are more consistent.

5. Conclusion

The conclusion is that PT. MEDISTA UTAMA has a fairly good maturity level for a company that has just started using information technology, but many upgrades are needed to maximize store performance and achieve the expected Maturity Level value. DS 5 Ensure Security System gets a maturity of 1.3 from expected 3, requires additional security on the data storage system used, requires an account to identify specific users and a special account as the main management account. DS 10 Manage Problems get a maturity value of 2 from the expected 3, the management can classify the problems experienced, find the best solution, and solve the problem well, but there is no formal procedure. DS 11 Manage Data got a maturity value of 2 from the expected 3, the management takes good care of the important data needed. Such as storing backup data and updating data regularly, but there is no formal procedure yet.

References

[1] Widiati, W., Studi, P., Akuntansi, K., & Selatan, J. (2016). Sistem Informasi Akademik Pada Sekolah Menengah Atas Swabumi. Vol IV No.1, Maret 2016. IV(1), 69–79.

[2] Widayanti, R., & Purnamawati, L. (2013). Audit Sistem Informasi pada aplikasi Sistem Manajemen Pemeriksaan (SMP) Badan Pemeriksa Keuangan Republik Indoenesia. Jurnal FIFO, 10(2), 262- 272.

[3] Andry, J. F. (2017). Audit Sistem Informasi Absensi Pada Pt. Bank Central Asia Tbk Menggunakan Cobit 4.1. Jurnal Teknik Informatika Dan Sistem Informasi, 3(2), 259–268.

[4] Andry, J. F. (2016). Audit Sistem Informasi Sumber Daya Manusia Pada Training Center Di Jakarta Menggunakan Framwork Cobit 4.1. Jurnal Ilmiah FIFO, 8(1), 42.

[5] Anderson, R., Kevin, K., & Andry, J. F. (2018). Audit Aplikasi Inventori Menggunakan Framework Cobit 4.1 Pada Store Nonna. It Journal Research and Development, 3(1), 1–12

[6] Andi, J. (2015). Pembangunan Aplikasi Child Tracker Berbasis Assisted – Global Positioning System (A-GPS) Dengan Platform Android. Jurnal Ilmiah Komputer Dan Informatika (KOMPUTA), 1(1), 1–8. elib.unikom.ac.id/download.php?id=300375

[7] Sukmajaya, I. B., & Andry, J. F. (2017). Audit Sistem Informasi Pada Aplikasi Accurate Menggunakan Model Cobit Framework 4.1 (Studi kasus Pt. Setia Jaya Tekhnologi). Seminar Nasional, 2(2502), 1–45.[7]Tika Pradini, J. F. A. (2018). Audit sistem informasi front office pada world hotel menggunakan kerangka kerja cobit 4.1. 2(Ikraith Informatika, Vol. 2, No. 1.), 1.

[8] Tika Pradini, J. F. A. (2018). Audit sistem informasi front office pada world hotel menggunakan kerangka kerja cobit 4.1. 2(Ikraith Informatika, Vol. 2, No. 1.), 1.

Author

Susi Susilowati
Lecturer of UBSI
susi.sss@bsi.ac.id